



CVE-2014-0083

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0083
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-21 14:15:00 UTC
Updated	2020-08-18 15:05:00 UTC
Description	The Ruby net-ldap gem before 0.11 uses a weak salt when generating SSHA passwords.

Risk And Classification

Problem Types: CWE-916

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Net-Ildap Project	Net-Ildap	All	All	All	All
Application	Net-Ildap Project	Net-Ildap	All	All	All	All

References

Reference	Source
Bug 863974 – VUL-1: CVE-2014-0083: rubygem-net-ldap: weak salt in password generation	MITRE
1065086 – (CVE-2014-0083) CVE-2014-0083 rubygem-net-ldap: SSHA passwords generated by the net-ldap Ruby gem use a weak salt	MITRE
Use SecureRandom to generate salt · ruby-ldap/ruby-net-ldap@b412ca0 · GitHub	CC BY
CVE-2014-0083	MITRE
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)